Refine Search

Search Results -

Terms	Documents
705/51	1027

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search:

Refine Search

Recall Text

Clear

Interrupt

Search History

DATE: Thursday, July 08, 2004 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L15	705/51	1027	L15
L14	705/74	136	L14
L13	705/65	359	L13
L12	705/26	4762	L12
L11	705/14	3523	L11
L10	705/42	584	L10
L9	705/38	908	L9
L8	705/36	1425	L8
L7	705/35	2003	L7
L6	705/39	1580	L6
L5	l1 and (anonymous or unknown or ghost) near transaction	115	L5
L4	L3 and issuance near2 prepaid	15	L4
L3	(negotiable near instrument or cash or credit near card)	84836	L3
L2	L1 and maintain$ near account	1280	L2

L1	(financial near institution or bank)	238298	L1

END OF SEARCH HISTORY

L5: Entry 101 of 115 File: USPT Feb 22, 2000

US-PAT-NO: 6029150
DOCUMENT-IDENTIFIER: US 6029150 A

TITLE: Payment and transactions in electronic commerce system

DATE-ISSUED: February 22, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Kravitz; David William	Albuquerque	NM		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Certco, LLC	New York	NY			02

APPL-NO: 08/ 726434 [PALM]
DATE FILED: October 4, 1996

INT-CL: [07] G06 F 17/60

US-CL-ISSUED: 705/39; 902/5, 380/24
US-CL-CURRENT: 705/39; 705/74, 705/75, 705/77, 902/5

FIELD-OF-SEARCH: 705/27, 705/26, 705/40, 705/39, 705/413, 705/44, 902/1, 902/2, 902/5, 902/24, 902/37, 380/24, 380/30

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4529870	July 1985	Chaum	
☐	4759063	July 1988	Chaum	
☐	4759064	July 1988	Chaum	
☐	4856061	August 1989	Thrane	380/48
☐	4914698	April 1990	Chaum	
☐	4926480	May 1990	Chaum	
☐	4947430	August 1990	Chaum	
☐	4949380	August 1990	Chaum	

☐	4987593	January 1991	Chaum	
☐	4991210	February 1991	Chaum	
☐	4996711	February 1991	Chaum	
☐	5131039	July 1992	Chaum	
☐	5276736	January 1994	Chaum	
☐	5373558	December 1994	Chaum	
☐	5434919	July 1995	Chaum	
☐	5448638	September 1995	Johnson et al.	705/413 X
☐	5453601	September 1995	Rosen	
☐	5455407	October 1995	Rosen	
☐	5485520	January 1996	Chaum et al.	
☐	5493614	February 1996	Chaum	
☐	5557518	September 1996	Rosen	
☐	5621797	April 1997	Rosen	
☐	5642419	June 1997	Rosen	
☐	5671280	September 1997	Rosen	
☐	5757917	May 1998	Rose et al.	705/26 X
☐	5768385	June 1998	Simon	380/24
☐	5794221	August 1998	Egendorf	705/40
☐	5809144	September 1998	Sirbu et al.	705/27 X
☐	5832089	November 1998	Kravitz et al.	705/39 X

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0 731 580	September 1996	EP	
0 693 742	January 1996	DE	
WO 96/13013	May 1996	WO	

OTHER PUBLICATIONS

Tang, "A Set of Protocols for Micropayments in Distributed Systems" First USENIX Workshop on Electronic Commerce pp. 107-115 Jul. 1995.
European Search Report, dated Mar. 12, 1998.
Marvin Sirbu, et al, NetBill: An Internet Commerce System Optimized for Network Delivered Services, Digest of Papers of the Computer Society Conference(Spring) Compcon, Technologies for the Information Superhighway San Francisco, Mar. 5-9, 1995, pp. 20-25.
Brickell et al., Trustee-Based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change, Proc, 6th Annual ACM-SIAM Symposium on Discrtet Algorithms, pp. 457-466, 1995.
Okamoto et al., Universal Electronic Cash, Crypto '91, NTT Laboratories, pp. 325-337.
Okamoto et al., Disposable Zero-Knowledge Authentications and Their Applications to

Untraceable Electronic Cash, Crypto '89, NTT Communications and Information Processing Laboratories, pp. 480-496.
Eng et al., Single-Term Divisible Electronics Coins, Eurocrypt '94, pp. 307-319.
David Chaum, Wallet Databases with Observers, Crypto '92, pp. 88-105.
David Chaum, Transferred Cash Grows in Size, Crypto '92, pp. 391-407.
"The First Virtual Solution", First Vitual, System Overview,Mar. 31, 1997, p. 1, http://www.fv.com/demo/.
The First Virtual Team, "Perils and Pitfalls of Practical Internet Commerce (Part I)", The Lessons of Fisrt Vitual's First Year, Company Information, First Virtual, Mar. 31, 1997, pp. 1-20, http://www.fv.com/company/first year1.html.
The First Virtual Team, Perils and Pitfalls of Practial Internet Commerce (Part II), The Lessons of First Virtual's First Year, Company Information, Mar. 31, 1997, pp. 1-34, http://www.fv.com/company/first year2.html.
Pays et al., "An Intermediation and Payment System Technology", Fifth International World Wide Web Conference, May 6-10, 1996, Paris, France, pp. 1-12, http://www/5conf.inria.fr/fich html/papers/P27/Overview.htm.
Alan Kotok, "GloblD Payment System", Nov. 1996, pp. 1-6, http://www.gctec.com/us/products/GlobelDPayment/gctechwhitepapers/globeidp ayment.htm.
"GobelD Payment: An Intermediation and payment system technology", p. 1 of 1, http://www.gctec.com/us/products/GlobelDPayment/gctechwhitw papers/wpglobeid.htm.
Cohen et al., "Electronic commerce: Beyond a simple change of medium", INET Ideas, May 1996, pp. 1-13, http://www.gctec.com/us/products/GlobelDPayment/gctechehitepapers/beyondch angeofmedium/3/31/91:ronicom.
"GlobelD Payment FAQ General issues", pp. 1-4, http:/www/gctec.com/us/products/GobelDPayment/GlobelDFAQ/globeidfaq.htm.
"GlobelD Payment model", p. 1 of 1, http://www.gctec.com/us/products/GlobelDPayment/globeidmodel.htm.
"FAQ about the GlobelD Technology", p. 1 of 7, http://www.gctec.com/us/Technical/FAQ.
Rivest et al.,"Payword and MicroMint: Two Simple micropayment schemes", Nov. 8, 1995, pp. 1-9.
Bellare et al., "iKP--A Family of Secure Electronic Payment Protocols", USENIX Association Firt USENIX Workshop on Electronic Commerce--Jul. 11-12, 1995.
J.D. Tygar, "Atomicity in Electric Commerce", 1996, pp. 8-26.
Sirbu et al., "NetBill: An Internet Commerce System Optimized for Network Delivered Services", The Netbill Overview, p. 1 of 2, http://www.ini.cmu.edu/netbill/pubs/ComCon TOC.htm.
NetBill: An Internet Commerce System Optimized for Netwoek Delivered Services:, The Netbill Overview, pp. 1-10, http://www.ini.cmu.edu/netbill/pubs/CompCon.htm#RTFToC.

Cox et al., "NetBill Security and Transcation Protocol", Carnegie Mellon University, USENIX Association First USENIX Workshop on Electronic Commerce--Jul. 11-12, 1995, pp. 77-87.
Neuman et al., "Requirements for Network Payment: The NetCheque TM Perspective", Information Sciences Institute University of Southern California, Proceeding of IEEE COMPCON '95, San Francisco, Mar. 1995.
Medvinsky et al., "Electronic Currency for the Internet", University of Southern California, Research Projects.
Medvinsky et al., "NetCash: A design for practical electronic currency on the Internet", Information Sciences Institute University of California.
"The Millicnet Protocol for Inexpensive Electronic Commerce", pp. 1-18, Nov. 8, 1996, http://www.research.digital.com/SRC/millicent/papers/millicent-w3c4/millic net.htm.
Mark S. Manasse, "The Millicnet protocols for electronic commerce", Systems Research Center, USENIX Association First USENIX Workshop on Electronic Commerce--Jul. 11-12, 1995, pp. 117-123, http://www.research.digital.com/SRC/people/Mark Manasse/bio.html.
David Chaum, Blind Signature System (Abstract), Crypto '83.

Stefan Brands, "Untraceable Off-line Cash in Wallet with Observers", Crypto '83, pp. 302-318.
Crepeau et al., "Discreet Solitary Games", Liens (CNRS URA 1327) and NEC Research Institute, 1992.
David Chaum, "Online Cash Checks", EUROCRYPT '89, Centre for Mathematics and Computer Science, pp. 288-293.
G. Brassard, University of Montreal, Protocols, Chaum et al., "Untraceable Electronic Cash", Crypto '88, pp. 319-327, Centre for Mathematics and Computer Science, Tel-Aviv University, IBM Almaden Research Center.
CMTM: The G.C. Tech Transaction Model, E-mail to"e-payment@cc.bellcore.com", Jul. 11, 1995.
The Globe ID Payment System, Globe ID, on Internet at "http://www.gctec.com".
An Intermediation and Payment System Technology, Fifth International World Wide Web Conference, May 6-10, 1996, Paris, France, on Internet at http://wwwconf.inria.tr/tich htm/papers/P27/Overview.html.
GCTech's Intermediation and Payment System Technology, Boston, Dec. 11, 1995, on Internet at http://www.gctec.com/us/Technical/Slides/Boston Pres/img05.html.
Electronic Commerce:Beyond a simple change of medium, Francis Cohen, et al, Jun. 1996, on Internet at http://www.gctec.com/us/Technical/Papers/INET/inetpaper.html.
Intermediation and Payment System Technical OverviewL Products & Services on Internet at http://www.gctec.com/us/Products/gol4.html.

ART-UNIT: 274

PRIMARY-EXAMINER: Kemper; Melanie A.

ATTY-AGENT-FIRM: IP Group of Pillsbury Madison & Sutro, LLP

ABSTRACT:

A method of payment in an electronic payment system wherein a plurality of customers have accounts with an agent. A customer obtains an authenticated quote from a specific merchant, the quote including a specification of goods and a payment amount for those goods. The customer sends to the agent a single communication including a request for payment of the payment amount to the specific merchant and a unique identification of the customer. The agent issues to the customer an authenticated payment advice based only on the single communication and secret shared between the customer and the agent and status information which the agent knows about the merchant and/or the customer. The customer forwards a portion of the payment advice to the specific merchant. The specific merchant provides the goods to the customer in response to receiving the portion of the payment advice.

47 Claims, 47 Drawing figures

Previous Doc Next Doc Go to Doc#

L5: Entry 101 of 115 File: USPT Feb 22, 2000

DOCUMENT-IDENTIFIER: US 6029150 A
TITLE: Payment and transactions in electronic commerce system

Brief Summary Text (7):
Financial Payments ($500K+): Transactions in this range are predominantly payments between financial institutions using electronic systems such as CHIPS, FedWire and SWIFT.

Brief Summary Text (14):
Cash transactions themselves are highly inefficient. Last year for example, Americans executed 300 billion cash transactions for items costing less than $20. Banks and businesses spend over $60 billion annually to move, secure, and account for these transactions. Growing numbers of consumers feel burdened by the inconvenience and risk in carrying cash. Further, it is currently impossible to use cash in the electronic marketplace.

Brief Summary Text (21):
In an off-line system, two parties exchange funds without any communication with a bank or other third party during the transaction. Off-line systems normally require hardware devices such as smartcards to provide adequate security. In order to download value (cash) onto the card, or to make a deposit, the card must be connected in some way to an electronic network to communicate with a bank or automated teller service. Until the device that receives a payment communicates with a bank over the network, the transaction is completely undocumented within the banking system.

Brief Summary Text (30):
There are electronic payment systems that are analogous to paper checks. An electronic check would typically consist of a document, signed by the payor using a certified digital signature key, which lists the information necessary for processing a paper check such as: the payor, the bank of the payor, the account number of the payor, the payee, the amount of the payment, and the date of the payment. The payee verifies the signature on the electronic check and then sends the electronic check to his bank for processing. The bank processing of an electronic check is essentially the same process as that used for paper checks today.

Brief Summary Text (31):
The advantage of electronic checks is that they take advantage of existing bank clearing processes, which reduces development time. In the basic model of electronic check, the payee would take the risk if the electronic check was not good. However, the merchant or payee would have two possible avenues to reduce his risk in the case of an on-line payment. If the bank was on-line, the payee could obtain approval from the bank that the check was good or he could require that the payor obtain a certified check from a bank.

Brief Summary Text (34):
There are numerous proposals for electronic payment systems that use electronic coins of fixed amounts as a means of exchange. A customer makes a withdrawal from his bank account and receives electronic coins from the bank. The customer can then

use these coins to pay a merchant. The merchant can check the validity of the coins using cryptographic techniques. Then the merchant can deposit the coins into the bank. Some electronic coin systems can be used with a multitude of banks.

Brief Summary Text (35):
An advantage of electronic coins is that a coin can be validated by cryptographic techniques so a merchant can be convinced that the coin is indeed valid. However, the merchant has no way to determine on his own whether the coin has been spent before. In order to determine this, the coin has to be given to the bank, and the bank has to check to see if that coin has been deposited before. Some systems suggest the use of tamper resistant hardware for storing the coins so that the tamper resistance has to be broken in order for the customer to spend a coin more than once.

Brief Summary Text (36):
There are electronic coin based systems that provide a very high degree of anonymity. Even if the banks and merchants pool their information about transactions, the identity of the payor of a particular transaction cannot be determined. Because this degree of anonymity might not be acceptable by some governments, there are electronic coin payment systems in which the identity of payors can be determined by trustees who could be independent of the banks and merchants.

Brief Summary Text (43):
Another approach to electronic payments uses devices that store a value on them. The device has a register in it that keeps an accounting of the amount of money stored in the device. A customer connects with a bank through an ATM or equivalent and withdraws money from his bank account and the value of the withdrawal is added to the register. The customer can authorize a movement of funds from his device to another device in the system. During this process, the value on his device is reduced and the value on the other device is increased by the same amount. In some systems, any device can accept payments, while in other systems only specified devices can accept payments.

Brief Summary Text (44):
An advantage of the stored value approach is that it requires little processing at the bank. Transactions can take place with no involvement from the bank.

Brief Summary Text (46):
There is another type of electronic payment that is strictly an off-line system using tamper resistant trusted devices. In this system, a device would have a signature key authorized by a bank. By taking the device to an ATM, or through some other communication with the bank, the customer can withdraw money from his bank account and the balance would be placed on the device together with an identifying number that is unique to this particular withdrawal. When the customer wants to pay a merchant, the device would use the signature key to sign an order to pay the merchant for a specified amount, the balance on the customer's device would be debited by that amount, and the balance on the merchant's device would be credited by that amount. There could be a multiplicity of balances on the customer's device.

Brief Summary Text (47):
One problem with this system is that it requires the bank to keep all records corresponding to a particular withdrawal until the entire withdrawal has been accounted for. Since the transactions could go to many merchants, all of these records must be held until all of the merchant's devices have been to an ATM.

Brief Summary Text (55):
Debit systems execute payment transactions by exchanging electronic tokens. These tokens are digitally signed by a participating bank and delivered to the consumer

in exchange for a debit to the consumers checking account. The debited funds are held in an escrow account, so that the amount of digital cash or tokens issued is backed by an equivalent amount of cash.

Brief Summary Text (57):
Debit systems are an attractive alternative to cash for many reasons. Transactions will occur faster because there is no need to wait for change. Debit systems eliminate the operational costs of handling cash. They improve security and reduce losses because businesses are able to transmit value to their bank at any time instead of having to wait for business hours to deposit cash.

Detailed Description Text (7):
Each customer has a bank 108, to which the CTA 102 is connectable via some standard mechanism such as an automated clearing house (ACH).

Detailed Description Text (10):
Merchant M has a bank 118 with which either the MCC 114 or the MCC's designated bank interacts via traditional financial networks 120. The merchant's bank 116 and the customer's bank 108 can be the same bank. The merchant M has an account with the MCC 114. The MCC 114 may designate accounts at one or more banks through which to execute payments to merchant banks 118 and/or to receive payments from customer banks 108, and/or there may be multiple MCCs 114. There may be multiple CTAs 102.

Detailed Description Text (11):
Preferably the CTA 102 is made up of a group of dedicated processors at a secure location. The CTA 102 executes electronic payments from customers to merchants within the system 100, as well as providing customer services such as database searches, records and customer receipts and allocation and/or collection of fees. The CTA 102 may designate an account at one or more banks through which to receive fees from customer banks 108.

Detailed Description Text (12):
The MCC 114, like the CTA 102, is preferably made up of a group of dedicated processors at a secure location. The MCC 114 collects and disperses funds due to merchants, possibly through the MCC's designated bank. The CTA 102 and the MCC 114 are not necessarily autonomous and may share accounts at designated banks.

Detailed Description Text (15):
First, in order to access the electronic transfer system 100, a customer C must subscribe to the service and establish an account within a particular CTA 102. This customer account must typically be funded before purchases can be made, for example through ATM 122, although actual funding is outside the scope of the payment system. The customer's bank 108 and the CTA 102 negotiate the availability of funds with respect to customer transactions within the payment system. The customer's bank 108 may send opening balances to the CTA 102 on some regular basis. The customer setup process is described in more detail below.

Detailed Description Text (17):
In response to receipt of the customer's digital payment request message 128 (step S208), the CTA 102 processes the request and, if the request is acceptable, executes an "intent to transfer" of funds from the customer C's account to the merchant M's MCC account (step S210). This intent to transfer has the characteristics of an exchange of cash in that it is instantaneous, final and non-appealable. The CTA 102 may perform certain checks during the process which may include a check that the CTA 102 has not been apprised that the designated merchant is not currently in good standing. At some point an actual transfer of funds is executed from the customer's bank 108 to the MCC 114 possibly into an account held by the MCC 114 at a designated bank. These fund transfers may be batched over multiple transactions per customer account and over multiple customer accounts for reasons of efficiency. The customer's bank 108 initiates these funds transfers in

response to detailed records and transfer requests it receives from the CTA 102. In a similar manner the MCC 114 may transfer refunds from a merchant's bank 118 to a customer's bank 108.

Detailed Description Text (21):
Payment records are forwarded routinely (e.g., daily) from the CTA 102 to the Merchant Clearing Corporation (MCC) 114 which provides a clearinghouse to manage merchant accounts. Merchants periodically receive the proceeds of all system payments by direct deposit from the MCC 114, or through an intermediary such as a bank designated by the MCC 114, into an account at a bank of their choice (merchant's bank 118).

Detailed Description Text (105):
A customer C sets up a system account at a participating bank 108 and is given a unique system account number.

Detailed Description Text (106):
The customer network software 104 is then delivered on a bank-provided diskette or is downloaded from a system distribution server over the public telephone network. A sixteen-digit long-term PIN is either delivered with the diskette or is mailed later by the bank 108 with the public key, described below. The long-term PIN is used for the distribution site's voice response unit (VRU).

Detailed Description Text (111):
The customer software uploads the public key to the system distribution server. The customer is also prompted to enter the customer's bank system account number. The distribution site and server are not part of the CTA 102. The server is preferably a direct-dial host. At end-of-day the distribution server sends a batch message to the CTA 102 listing all newly applied-for account numbers. The CTA 102 creates an internal account flagged inactive and sends an out-of-band batch message to the bank 108 listing all accounts to be approved.

Detailed Description Text (112):
The bank 108 returns to the customer a physical form (typically a fax or postal letter) containing the customer's hashed public key. The customer compares the delivered hashed public key to a readable version of the hashed public key already stored in the customer's software. The two hashes must match in order to be valid. The customer signs the physical form and returns it through regular postal mail to the bank 108. The bank 108 performs a physical signature verification, which binds the public key to the customer's identity.

Detailed Description Text (113):
Routinely, e.g., nightly, the bank 108 sends a batch transfer of all verified, rejected, and revoked accounts to the CTA 102. Upon receipt of the verification message, the CTA 102 binds the public key to the customer's account number and activates the customer's account.

Detailed Description Text (324):
information about one or more transfers from the customer's bank into his CTA account, i.e., fundings information (Funding Information Message 188, FIG. 7L);

Detailed Description Text (327):
External evidence acts to attach identity to a previous anonymous transaction with a merchant. That is, it serves as a means to re-contact a merchant via the CTA 102, regarding, for example, a transaction for which the payment advice may or may not have reached the merchant, but the merchant was credited for the transaction.

Detailed Description Text (329):
In the preferred embodiment, the notification to the merchant occurs whether or not a refund has been requested of the merchant and/or processed. Notifications to the

merchant may be aggregated and delivered as part of the regular merchant-transaction statement (or as a separate statement). A successfully executed external evidence request results in a CTA-signed binding of the original transaction information to the customer's account information as it is known to the CTA 102. In the preferred embodiment, the notification to the merchant regarding an external evidence request does not include the customer's account information. Furthermore, the association of the account to the person's actual name or other bank-held information must be provided by the bank. This proof-of-association may be provided to the customer as part of the hard-copy documentation delivered to the customer as part of customer setup. In this case, the customer must retain a bank-authenticated original copy of the document, which may later be provided to a third party if necessary. Alternatively, the customer may be required to acquire such documentation from his bank on an as-needed basis.

Detailed Description Text (413):
The detailed statement, showing each payment received, is sent to the merchant via some form such as electronic mail. When electronic mail is used, the merchant may select any electronic mail address for delivery of the mail, including, e.g., his Internet server's address. The merchant network server 110 allows merchants to request a new copy of the last detailed statement received. Statements are sent to the merchant via electronic mail. The detailed merchant statement and complete records maintained on the merchant network (Internet) server may be used to verify accuracy of each payment. Individual payments may be matched by the merchant identifier and merchant transaction identifier. The merchant's bank statement should contain a payment in the amount matching the total indicated in the detailed statement from the MCC 114.

Detailed Description Text (441):
In another embodiment, customers and merchants can have pre-established relationships. For example, a merchant may be a local utility company or a telephone company. The customer may then set up a pre-authorized payment from his bank to the merchant, the payment being triggered by the merchant's receipt of a payment advice from the customer. In this case the payment advice takes on a more general function of notifying a merchant that it can initiate the pre-authorized payment.

Detailed Description Text (442):
In some embodiments, the customer establishes a pre-authorized payment with an upper limit, for example, $200. Then the quote from the merchant specifies the actual amount that the customer must pay. When the customer obtains a payment advice from the agent and forwards it to the merchant, this payment advice authorizes the merchant to initiate the transfer of the actual amount from the customer's bank to the merchant's bank.

Previous Doc Next Doc Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

Generate Collection Print

L5: Entry 102 of 115 File: USPT Jun 15, 1999

US-PAT-NO: 5913203
DOCUMENT-IDENTIFIER: US 5913203 A

TITLE: System and method for pseudo cash transactions

DATE-ISSUED: June 15, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Wong; Jacob Y.	Santa Barbara	CA		
Anderson; Roy L.	Glendale	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Jaesent Inc.	Goleta	CA			02

APPL-NO: 08/ 720785 [PALM]
DATE FILED: October 3, 1996

INT-CL: [06] G06 F 17/60

US-CL-ISSUED: 705/39; 705/26, 705/43
US-CL-CURRENT: 705/39; 705/26, 705/43

FIELD-OF-SEARCH: 705/6, 705/39, 705/43, 705/44, 705/26, 380/24, 380/25, 380/4, 364/479.02

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	3665161	May 1972	Oberhart	235/379
☐	3845277	October 1974	Voss et al.	235/379
☐	4016405	April 1977	McCune et al.	235/380
☐	4234932	November 1980	Gorgens	235/379
☐	4314352	February 1982	Fought	235/379
☐	4390968	June 1983	Hennessy et al.	380/24
☐	4438326	March 1984	Uchida	705/43

☐	4650978	March 1987	Hudson et al.	235/380
☐	4755940	July 1988	Brachtl et al.	705/44
☐	5220501	June 1993	Lawlor et al.	380/24
☐	5371797	December 1994	Bocinsky, Jr.	380/24
☐	5373558	December 1994	Chaum	380/23
☐	5434919	July 1995	Chaum	380/30
☐	5438186	August 1995	Nair et al.	235/449
☐	5440108	August 1995	Trean et al.	235/381
☐	5444616	August 1995	Nair et al.	705/17
☐	5448047	September 1995	Nair et al.	705/35
☐	5455407	October 1995	Rosen	380/24
☐	5850442	December 1998	Muftic	380/21

OTHER PUBLICATIONS

International Search Report re PCT/US97/15701.
Article from Scientific American entitled "Achieving Electronic Privacy" by David Chaum, Aug. 1992; pp.. 96-101.
Article entitled "Security Without Identification: Transaction Systems to Make Big Brother Obsolete" by David Chaum, Communications of the ACM; vol. 28 No. 10; Oct. 1985; pp. 1030-1044.
Article entitled "Online Cash Checks" by David Chaum, Advances in Cryptology EUROCRYPT '89; J.J. Quisquarter & J. Vanderwalle (Eds.), Springer-Verlag; pp. 288-293.

ART-UNIT: 275

PRIMARY-EXAMINER: MacDonald; Allen R.

ASSISTANT-EXAMINER: Jeanty; Romain

ATTY-AGENT-FIRM: Lyon & Lyon LLP

ABSTRACT:

Totally anonymous or effectively anonymous cash-like transactions are accomplished by using a pseudo cash data package converter for inserting a user key into a pseudo cash preliminary data packet through the use of a user insertion key to generate a pseudo cash unit with a fixed monetary value that can be used to purchase goods or services via the Internet. A pseudo cash repository facilitates the cash-like transactions and maintains a record of the pseudo cash units and their fixed monetary value. Depending upon the level of anonymity selected by a purchaser, the pseudo cash repository can either transmit pseudo cash preliminary data packets or pseudo cash units to a first entity. If the first entity loses an effectively anonymous pseudo cash preliminary data packet, it can be replaced by the pseudo cash repository without risk of loss.

71 Claims, 3 Drawing figures

Previous Doc Next Doc Go to Doc#

L5: Entry 102 of 115 File: USPT Jun 15, 1999

DOCUMENT-IDENTIFIER: US 5913203 A
TITLE: System and method for pseudo cash transactions

Brief Summary Text (7):
Another concept called "Cybercash" requires customers or buyers on the Internet to first open a special Cybercash bank account that contains money designated for spending on the Internet. A consumer issues instructions to purchase goods or services on the Internet and money for these items are transferred from the consumer's Cybercash bank account to that of the merchant's. Transactions are anonymous unless the seller specifically asks for the identity of the buyer. Again one can readily see that this concept, although rather secured from the money handling standpoint, is not totally anonymous. Furthermore, it is rather complicated involving a number of interactions between the buyer, the Cybercash bank and the seller. It is definitely incompatible with the simple elegance of doing shopping on the Internet, particularly with regards to speed and ultimate privacy.

Brief Summary Text (10):
The best system to date, but by no means perfect or totally practical, is the so-called "Digicash" or "ecash". In theory this system turns a user's or buyer's hard drive on a PC into a purse. To use this system, one first establishes an account with a bank. To obtain digicash or ecash, the user creates a series of numbers that will represent a mixture of coins or money bills in various denominations according to the user's own wishes. This request for digicash is then sent to the bank, which deducts the total amount requested from the user's existing valid account. The bank then sends the user an equivalent amount of ecash as an encrypted email message containing a series of numbers. Each number corresponds to a specified amount of money.

Brief Summary Text (11):
Before the user can actually use these encrypted series of numbers from the bank to purchase goods or services on the Net, the user must first obtain a user name and a password from Digicash. Then the user has to download Digicash's ecash software to the user's PC. The final step is to create the user's own encryption key (in essence another password) and together with the user's password obtained earlier from Digicash, the user can then spend ecash on the Net.

Brief Summary Text (13):
Second, as implemented today, the Digicash system is very interaction intensive and rather loosely organized. Requests by users to the bank and the bank's handling of their requests alone could be an awesome burden to the bank when the traffic builds up in a hurry. This is especially the case when there is no amount limits of any kind imposed on any ecash request. Thus a one dollar request must be handled in the same way as one that is for $1,000.

Brief Summary Text (14):
Third, even though the anonymity for any transaction is strong, it is by no means absolute. The reason is that the encrypted ecash that is passed on to a user originates from a bank who has the account information of the individual. In order that the bank subsequently honors this particular ecash from the merchants, it

needs to reconcile with its initial issuance and that leads to the original account that requested it.

Brief Summary Text (22):
In yet another, separate aspect of the present invention, the first entity receives a pseudo cash unit generated by the pseudo cash repository in exchange for the fixed monetary value associated with the pseudo cash unit. The pseudo cash repository maintains an active record of the pseudo cash unit until the pseudo cash unit is exchanged for the fixed monetary value. Because the identity of the first entity cannot be determined from any record maintained by the pseudo cash repository, the transaction is an anonymous transaction similar to an anonymous cash transaction.

Detailed Description Text (3):
Initially, there must be a money source. This is described as a pseudo cash repository, but it does not need to be a single entity. In practice, it can be a single bank, or a single credit card company or a number of affiliated banks (a bank group) or a number of affiliated credit card companies (a card group) affiliated with one or more merchants and set up to do business with one or more money source customers or some other entity or entities that will perform such a function. The pseudo cash repository, in concept, is similar to an entity that issues traveler's checks (for a non-anonymous cash-like transaction) or a money order (for a potentially anonymous cash-like transaction).

Detailed Description Text (5):
There is no limit to how many customers and merchants a single bank, a single credit card company, one or more banks within a bank group or multiple bank groups, or one or more credit card companies within a card group or multiple card groups can have within the system structure. Similarly, a customer can affiliate with a single bank, a single credit card company, one or more banks within a bank group or multiple bank groups, one or more credit card companies within a card group or multiple card groups, or any combinations thereof within the system structure. Also, a merchant can affiliate with a single bank, a single credit card company, one or more banks within a bank group or multiple bank groups, one or more credit card companies within a card group or multiple card groups.

Detailed Description Text (7):
The pseudo cash dispenser dispenses a pseudo cash preliminary data packet or a pseudo cash unit in exchange for a fixed monetary value. A pseudo cash preliminary data packet is a string of characters, preferably eight or more. The characters, for convenience, are either letters of the alphabet or numerals, but other characters could also be used without departing from the spirit of the invention. The pseudo cash dispenser can dispense the pseudo cash preliminary data packet to the first entity by any suitable means. If the pseudo cash preliminary data packet is dispensed by an automated teller machine, the string of characters could be printed on a receipt in the same fashion that account balances and other information are commonly available to bank customers in the United States today by automatic teller machines. The pseudo cash preliminary data packet could also be dispensed over an electronic communication medium, such as the Internet or a telephone line.

Detailed Description Text (20):
Further details of the systems and methods of the preferred embodiment will now be described. For ease of description, it will be assumed that the pseudo cash repository is a bank.

Detailed Description Text (21):
With reference to FIG. 3, the bank obtains the usual personal information from the customer and establishes a certain amount of credit for the customer according to the customer's personal financial condition. According to the present system, the

bank will also issue the customer an account number, a user key and a user insertion key. Because the user key is similar to the concept of a personal identification number (PIN) presently in common use, the user key will hereinafter be referred to as PIN and the user insertion key will hereinafter be referred to as a PIN insertion sequence number (PISN). The customer may also pick his or her own PIN and PISN so that the customer can remember these numbers and use them without having to look them up. There is no difference in the use of the PIN number between the current banking practice and the present system. Normally the customer uses this PIN to obtain cash from his or her bank account at ATMs and for other private financial transactions with the bank. The present system has similar ideas.

Detailed Description Text (22):
The PIN insertion sequence number or PISN on the other hand is a distinct feature of the present Internet cash dispensing system. Together with the PIN, these two numbers constitute the private "Key" to the customer's bank account in the system. Whereas the PIN is typically a 4 or 5 character numeric number in ordinary bank usage, in the current system, the PIN can be any number of alpha-numeric digits, preferably not less than four (4).

Detailed Description Text (28):
There are two categories of Internet cash identified by the current cash dispensing system according to their level of anonymity. Category I (Cat I) cash refers to pseudo cash units created by the system that absolutely cannot be traced. Category II (Cat II) cash refers to pseudo cash units created by the system that can only be traced through the bank of origin, or the nerve center. Consequently, Internet cash generated and used in the current system can generally be considered anonymous. Furthermore, for this reason a special name has been chosen for the presently invented cash dispensing system for the Internet. It is called System for Processing Electronic Cash Transactions Anonymously or the SPECTA system.

Detailed Description Text (29):
Referring again to FIG. 1, a person can walk into a bank and use real cash to purchase Category I cash from the bank using the SPECTA system. In this case the bank simply issues the person the Cat I cash in exchange for real cash. Example: A person wishes to purchase $200 Internet Cat I cash in the following denominations:

Detailed Description Text (30):
The bank issues the person the following Cat I Internet cash as follows:

Detailed Description Text (31):
Needless to say, as the bank issues these Cat I Internet cash, it only keeps track of what Cat I cash or codes have been issued without having to inquire about the purchaser's personal information or references. In essence, this is just a cash transaction. Thus, these Cat I cash are just like real cash and any person who has access to these Cat I codes will in fact be the owner of these cash. If these Cat I cash are lost or misplaced, or the codes are revealed to a stranger, then it is like losing the cash and the original purchaser might never be able to recover these Internet negotiable cash.

Detailed Description Text (32):
From the System standpoint, as these Cat I cash are issued, the bank will immediately create a record of these Cat I codes with their associated monetary value. Note that these Cat I codes (or "keyed" Cat II codes, see below) are stored for verification purposes only and they are not available for inspection or revelation to anybody. Thus the purchaser can indeed spend these Cat I cash on the Internet as negotiable cash without any restriction except that the merchants have to be affiliated with the same money source from which the Internet cash was purchased. The purchaser can in fact purchase Cat I cash from the bank in any amount with real cash if the customer knows ahead of time exactly how much Internet cash the customer will need, for example like $125.78.

Detailed Description Text (33):
Now referring to FIGS. 1 and 3, a person can walk in and purchase Cat I cash from the bank using a bank account or credit instead of real cash. The bank can issue the customer the same Cat I cash codes as before without having to link the customer in any way to these Internet cash.

Detailed Description Text (34):
The customer can also use the customer's bank account or credit to purchase Cat II cash. Since the bank knows and can use the customer's private "Key" at the bank, the Cat II cash can be issued to the customer on site in a simpler form, as pseudo cash preliminary data packets, as follows (same example of $200 as before):

Detailed Description Text (35):
Furthermore, the customer can even have the bank send these Cat II codes to the customer's email address on the Internet without risking anything. (In this latter case, the customer might just as well use a regular phone to call up the bank instead of showing up at it to do the transaction.) Note that the Cat II codes only contain eight (8) alpha-numeric characters instead of 12 like the Cat I cash or codes. By giving up absolute anonymity, Cat II cash is much more secured. It is because the Cat II codes themselves are not negotiable on the Internet as they are issued. The purchaser in this case must "key" these Cat II codes using his or her personal "Key" (see example given earlier) in order to turn them into 12-character Cat II Internet cash. Since the customer's "Key" is private and the customer does not have to "key" the Cat II codes to convert them into Cat II cash until the very last minute when the customer needs the cash on the Net, the customer can treat these Cat II codes with much less care. But the bank knows the customer's "Key" and it must convert the Cat II codes into Cat II cash to create an active record 12 for each Cat II code. Thus even if these Cat II codes are lost or misplaced, nobody can take advantage of them and the purchaser can retrieve them from the bank with information linking to the customer's bank or credit card account.

Detailed Description Text (36):
The SPECTA system does not specify the nature and characteristics of the encrypted communication link between the money source and its affiliated merchants or bank members. Such communication links can vary all the way from digital phone lines like the Integrated Services Digital Network (ISDN), digital cellular radio network using advanced satellite systems, or even the Internet network itself. At the same time the encryption method could use any on-the-fly encryption technology ranging from 64- to 128 bit or any future enhancement implementation. The purpose for not specifying the exact nature and characteristics of the encrypted link for the system is to allow for future technological advancement in this area without any impact to the systems's operation. Thus, it is up to the nerve centers of this system to take advantage of any performance enhancement and cost reduction in this area in order to minimize the overall system transaction costs.

Detailed Description Text (38):
Referring to FIG. 3, a person with an email address on the Internet can purchase Cat II cash from the money source using the Internet alone. The only requirement is that the person has to "key" his or her bank or credit account number with his or her private "Key" before forwarding it to the bank's email address with any messages or requests. Like before, the bank will email the customer the Cat II codes and make activate a record of Cat II cash. Everything is exactly the same as in the previously illustrated examples.

Previous Doc Next Doc Go to Doc#

L5: Entry 110 of 115 File: USPT Jun 23, 1998

US-PAT-NO: 5770844
DOCUMENT-IDENTIFIER: US 5770844 A

TITLE: Supervision of transactions with chip cards

DATE-ISSUED: June 23, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Henn; Horst	Boeblingen			DE

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Business Machines Corporation	Armonk	NY			02

APPL-NO: 08/ 736888 [PALM]
DATE FILED: October 25, 1996

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
DE	195 39 801.7	October 26, 1995

INT-CL: [06] G06 K 5/00

US-CL-ISSUED: 235/380; 235/379, 902/26
US-CL-CURRENT: 235/380; 235/375, 235/379, 902/26

FIELD-OF-SEARCH: 235/379, 235/380, 902/26

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	3852571	December 1974	Hall et al.	235/379

ART-UNIT: 254

PRIMARY-EXAMINER: Pitts; Harold

ATTY-AGENT-FIRM: Hesse; K. O. Seaman; K. A.

ABSTRACT:

A transaction audit system is disclosed comprising a chip card, for completing a transaction between the holder of the chip card and a transaction partner such as a merchant. During the transaction, a transaction identifier is generated uniquely identifying the transaction. For completing execution of the transaction by posting of the payment amount to the merchants account, the chip card transmits a transaction receiver data record comprising the transaction identifier, and further data, if required, to a third party. To allow auditing the transaction settlement posting accuracy, the transaction provider also transmits a transaction provider data record comprising the corresponding transaction identifier to the third party. The third party is then able compare the receiver data record and the provider data record and identify possible irregularities, such as possible errors or manipulations in the transaction system, or intentional or non-intentional manipulation by the participants to the transaction, particularly the transaction receiver. The transaction identifier identifies both the transaction receiver data record and the transaction provider data record as being data records belonging to the same transaction.

13 Claims, 2 Drawing figures

Previous Doc Next Doc Go to Doc#

L5: Entry 110 of 115 File: USPT Jun 23, 1998

DOCUMENT-IDENTIFIER: US 5770844 A
TITLE: Supervision of transactions with chip cards

Brief Summary Text (5):
Chip cards are used today, among other things, for payment of money without the transfer of cash or checks. For that purpose, the chip card comprises a purse into which a certain amount of money may be stored. On payment at a cashier or a respective automatic machine, the amount of money to be paid is transferred from the chip card of the customer providing the money to the receiver of the money, such as a merchant. As a rule, in such a transaction the purse of the customer is reduced by a certain amount and such amount is credited to the merchant or other transaction partner. The transaction partner then balances accounts directly or indirectly with the bank which credits the amount to the partners account.

Brief Summary Text (7):
In the use of purses on chip cards a distinction must be made between the so-called anonymous and non-anonymous purses. In the case of non-anonymous purses, the chip card transmits a respective individual identifier which is characteristic for this particular chip card during a transaction with this transaction partner. For such transaction a transaction data record is created which enables a merchant transaction partner to settle the transaction with a bank in order to obtain the amount of money as credit on the merchant account. A non-anonymous transaction data record includes information related to the chip card, the record permits directly correlating the transaction back to the chip card and thereby to the holder of the chip card. Therefore modes of behavior of the chip card holders may be derived from a plurality of transaction data records. Such correlation is undesirable from the perspective of data and privacy protection.

Brief Summary Text (8):
In the case of anonymous purses, however, the chip card does not furnish an identifier identifying the chip card during the transaction with the transaction partner. However, in a transaction using an anonymous purse, a data record will be created as before, which enables a merchant transaction partner to settle the transaction accounts with a bank. The transaction data record does, however, not permit an attacker to correlate the transaction back to the holder of the chip card and thereby identify the holder or perpetrate a fraudulent transaction using the holders identity. Anonymous purses are today preferred for reasons of data protection, since the monitoring and reproducing of the customer's behavior is not possible.

Brief Summary Text (9):
In the prior art, a chip card is read by a chip card reader, of a transaction partner, such as a merchant. During the transaction a transaction data record TD is created which enables the transaction partner to settle the accounts of the transaction. The transaction partner establishes an immediate connection with a communication port of a bank computer 35, either directly through a settlement transmission path 40 or indirectly, and transfers the transaction data record to the computer 35 for settling the accounts of the transaction. The respective amount corresponding to the transaction is then credited to the transaction partner. The amount has already been debited from the purse of the chip card and earlier debited

from an account of the customer when the balance in the chip card purse was loaded or raised.

Brief Summary Text (10):
In today's usual bank payment transaction system, using checks or remittances, the customer monitors account settlement posting accuracy by reviewing each month end statement. The customer himself has a vital interest in determining that his payments are correctly settled. On the basis of the statements of account or the paid checks, the customer has the possibility of checking the accuracy of the payments and transactions. By this means a reasonable audit of the payment transaction system is obtained.

Brief Summary Text (18):
Generally, in each transaction there are at least one transaction provider and at least one transaction receiver. The transaction provider transfers something, such as an amount of money, to the transaction receiver, and the transaction receiver intends then to process the transaction generally with a third party, such as a bank or another participant in the transaction system, in which the transaction is carried out. In this context it is to be understood that everyone participating in the transaction may be both transaction provider and transaction receiver. The one participant in the transaction who wants to claim the monetary proceeds of the transaction for himself, i.e. the transaction receiver, must have the transaction identifier for completing settlement the transaction.

Brief Summary Text (19):
For completing the execution of the transaction, the transaction receiver transmits a transaction receiver data record which contains a transaction identifier and other data to a third party such as a bank. The transaction receiver data record permits the bank to complete the monetary transfer of the transaction by carrying the data required for settlement. The transaction identifier substantially serves to identify the transaction and, if required, also for proving that the transaction participants, also known as the transaction provider and the transaction receiver, are authorized participants within the system in which the transaction is carried out. It will be understood that the transaction receiver record may be identical with the transaction identifier if the transaction identifier already carries enough information to enable execution of the settlement steps of the transaction.

Detailed Description Text (7):
Referring now to FIG. 2, during the payment transaction event, a merchant identifier HI of the merchant and the amount B to be deducted from the chip card 10 are transferred from the computer 25 of cashbox 20 to the computer 15 of chip card 10 at block 105. From the chip card 10, the random value V2 is transmitted to the cashbox 20 of the merchant as shown in block 107. In the cashbox 20 of the merchant, a transaction identifier is generated by computer 25 at block 109 which includes the merchant identifier HI and the amount and the created random value V2. The transaction identifier marks the payment transaction event between the chip card 10 and the merchants cash box 20. The random value V2 indicates during the following settling of accounts, whether the chip card 10 and the merchants cash box 20 are valid parties in the payment system. The transaction identifier is placed into a merchant data record DH at block 111 which may contain yet other data or in which a plurality of various payment events are combined. The merchant data record DH comprises the merchant identifier HI and of pairs B(1)-V2(1), B(2)-V2(2), . . . , B(i) being thereby the amount of the i-th event and V2(i) symbolizing the i-th random value. All payments are documented in that merchant data record DH. If 8 bytes are added to the merchant identifier and the amount B and the random value V2 are encrypted each with 4 Bytes, 255 payment events may be protocolled by one kilobyte. This merchant data record DH is transferred by the merchant at block 125 to the supervising facility 30 such as a bank terminal having a computer 35 for settling the accounts. The transfer of the data record DH may be carried out on-line through transmission path 40 or also by means of a special chip card for

storing payee data. It is recognized that paths 40 and 50 can be either physical telecommunication lines or alternately can be transceivers such as used in cashbox 20 for communicating with chip cards.

Detailed Description Text (14):
While the invention has been shown and described with respect to the preferred embodiment, it will be understood by those skilled in the art of system design that various changes may be made without departing from the spirit and scope of the invention as measured by the following claims. For example simplified auditing of payment transactions according to the invention may be carried out between two or more chip cards participating in a payment transaction. In such case, the merchant data record DH is stored in a merchant chip card and is transmitted during a next `on-line` contact with the supervising bank device 30 for factual settlement, such as by a credit note or a refill of a purse on the merchant chip card.

Previous Doc Next Doc Go to Doc#